HIPAA - Privacy – Minimum Necessary

TRICARE Management Activity, Electronic Business Policy & Standards

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996 (HIPAA)

January 2003
OSD(HA), TMA eBPS

Highlights

- General Requirement
- Uses & Disclosures of, and Request for, PHI
- Reasonable Reliance
- De-Identified Information

General Requirement

The Privacy Rule generally requires covered entities to take reasonable steps to limit the use or disclosure of, and request for protected health information (PHI) to the minimum necessary to accomplish the intended purpose. The minimum necessary standard is intended to make covered entities evaluate their practices and enhance protections as needed to limit unnecessary or inappropriate access to, and disclosures of, PHI. The minimum necessary provisions do not apply, however, to the following:

- Disclosures to or request by a health care provider for treatment purposes
- Disclosures to the individual who is the subject of the information
- Uses and disclosures made pursuant to an authorization requested by the individual
- Uses and disclosures required for compliance with the standardized HIPAA transactions.
- Disclosures to the Department of Health and Human Services (HHS) when disclosure of information is required under the rule for enforcement purposes
- Uses or disclosures that are required by other law.

Uses & Disclosures of, and Request for, PHI

For uses of PHI, the MTF's policies and procedures must identify the persons or classes of persons within the covered entity who need access to the information to carry out their job duties, the categories or types of PHI needed, and conditions appropriate to such access. For example, hospitals may implement policies that permit doctors, nurses, or others involved in treatment to have access to the entire medical record as needed. Case-by-case review of each use is not required. Where the entire medical record is necessary, the covered entity's policies and procedures must state so explicitly and include a justification.

For routine or recurring requests and disclosures as described in the Notice of Privacy Practices, the policies and procedures must limit PHI disclosed or requested to that which is the minimum necessary for that particular type of disclosure or request. Individual review of each disclosure or request is not required.

For non-routine disclosures, covered entities must develop reasonable criteria for determining, and limit disclosure to, only the minimum amount of PHI necessary to accomplish the purpose of a non-routine disclosure. Non-routine disclosures must be reviewed on an individual basis in accordance with these criteria. When making non-routine requests for PHI, the covered entity must review each request so as to ask for only that information reasonably necessary for the purpose of the request.

HIPAA PROGRAM OFFICE

Skyline 5, Suite 810
5111 Leesburg Pike
Falls Church, VA
22041-3206
Ph: 703-681-5611
Fax: 703-681-8845

TMA HIPAA Website:
www.tricare.osd.mil/hipaa

E-Mail:
hipaamail@tma.osd.mil

TRICARE Management Activity

Reasonable Reliance

In certain circumstances, the Privacy Rule permits a covered entity to rely on the judgement of the party requesting the disclosure as to the minimum amount of information that is needed. Such reliance must be reasonable under the particular circumstances of the request. This reliance is permitted when the request is made by:

- A public official or agency for a disclosure permitted under the Privacy Rule
- Another covered entity
- A professional who is a workforce member or business associate of the covered entity holding the information

The rule does not require such reliance, however, and the covered entity always retains discretion to make its own minimum necessary determination for disclosures to which the standard applies.

De-Identified Information

To ensure only the minimum necessary information is provided to third parties, certain data sets may need to be removed. The Privacy Standards do not protect health information that has been "de-identified" by removing, coding, encrypting or otherwise eliminating or concealing all individually identifiable health information. De-identified information may be used or disclosed freely as long as no means of re-identification is disclosed. If de-identified information is re-identified, permission to use or disclose is required.

To properly de-identify information, HIPAA requires the removal of the following identifiers with respect to the individual, his or her relatives, employers and household members.

- Names
- Geographic subdivisions smaller than a state
  - Address
  - City
  - County
  - Precinct
  - Zip code or equivalent geocode
- All elements of dates (except year) for dates related to an individual
  - Birth date
  - Admission date
  - Discharge date
  - Date of death
  - All ages over 89
  - All elements of dates (including year) indicative of age, except an aggregated single category of "90 or older" is permissible
- Social Security Number
- Telephone numbers
- Fax numbers
- E-mail address
- Universal Resource Locator (URL)
- Internet Protocol (IP) address
- Medical record number
- Health plan beneficiary number
- Account number
- Certificate/license number
- Vehicle identifiers, serial numbers and license plate numbers
- Device identifiers and serial numbers
- Biometric identifiers, voice and fingerprints
- Full face photographs and comparable images